

HOMEWORK 7

~~DUE FRIDAY, NOVEMBER 22~~ WEDNESDAY, NOVEMBER 27, 2024 AT 11:59PM

The homework is due in Gradescope at the stated time. You may submit handwritten text (scanned from paper or written on a tablet) or a typed PDF (e.g., created using LaTeX). If you choose the handwritten option, you have to also submit a hardcopy in class or put it in my mailbox.

Collaboration and research is fine, as long as you do the following.

- Try the problems yourself first!
- Write the solutions in your own words.
- Acknowledge all sources and collaborators.

1. Let K be the number field $\mathbb{Q}(2^{1/4})$. Let L be the Galois closure of K and $G = \text{Gal}(L/K)$.
 - (a) Prove that L is the splitting field of the polynomial

$$x^8 - 4x^6 + 8x^4 - 4x^2 + 1.$$

This is the field <https://www.lmfdb.org/NumberField/8.0.16777216.2>.

In terms a root a of this polynomial, a $\mathbb{Z}$ -basis for $\mathcal{O}_L$ is

$$1, a, a^2, a^3, a^4, a^5, \frac{1}{3}a^6 + \frac{1}{3}a^4 + \frac{1}{3}a^2 + \frac{1}{3}, \frac{1}{3}a^7 + \frac{1}{3}a^5 + \frac{1}{3}a^3 + \frac{1}{3}a.$$

- (b) Check that there is a single prime $\mathfrak{q}$ of L above 2 and that $\mathfrak{q}$ is totally ramified over 2.
 - (c) Compute the groups $G_{\mathfrak{q},s}$ for all s .
 - (d) Use the answer to (c) to compute the different of $L/\mathbb{Q}$.
2. Show that every quadratic extension of $\mathbb{Q}_2$ is contained in $\mathbb{Q}_2(\zeta_{24})$. (Hint: first compute $\mathbb{Q}_2^*/(\mathbb{Q}_2^*)^2$.) This is a first step towards the Kronecker-Weber theorem, which will be discussed in more detail in Math 204B.
3. Let L/K be an extension of number fields. Let $\mathfrak{p}$ be a prime ideal of K and suppose that there is a unique prime ideal $\mathfrak{q}$ of L above $\mathfrak{p}$. Let $\alpha \in \mathcal{O}_K$ be an element whose image in $\mathcal{O}_L/\mathfrak{q}$ is a primitive element over $\mathcal{O}_K/\mathfrak{p}$.
 - (a) Let $P(T) \in \mathcal{O}_K[T]$ be a monic polynomial whose reduction modulo $\mathfrak{q}$ is the minimal polynomial of α over $\mathcal{O}_K/\mathfrak{p}$. Show that there exists $\beta \in \mathcal{O}_L$ congruent to α modulo $\mathfrak{q}$ such that $P(\beta) \in \mathfrak{q} \setminus \mathfrak{q}^2$. (Hint: use the first-order Taylor expansion of P at α , as in the proof of Hensel's lemma.)

- (b) For β as in (a), prove that $\mathcal{O}_{L,\mathfrak{q}} = \mathcal{O}_{K,\mathfrak{p}}[\beta]$. (This is Lemma II.10.4 of Neukirch, but try it yourself first.)
4. Let L/K be a Galois extension of number fields of degree n . Let $\mathfrak{q}$ be a prime ideal of L lying above the prime ideal $\mathfrak{p}$ of K .
- (a) Prove that the $\mathfrak{q}$ -adic valuation of the different of L/K is at most $e - 1 + v_{\mathfrak{q}}(e)$ where $e = e(\mathfrak{q}/\mathfrak{p})$. (Hint: reduce to the case where $e = [L : K]$, then look at the minimal polynomial of an element of $\mathfrak{q} - \mathfrak{q}^2$. If you get stuck, see Theorem III.2.6 of Neukirch.)
- (b) Use (a) to prove that for any fixed positive integers n and D , there are only finitely many number fields of degree n with discriminant $\pm D$. Recall that this was the missing step in the proof of the Hermite-Minkowski theorem.
5. (a) Let K be a field complete with respect to a nonarchimedean absolute value. Let $P(T) \in \mathcal{O}_K[T]$ be a polynomial, and suppose $\alpha \in \mathcal{O}_K$ satisfies

$$|P(\alpha)| < |P'(\alpha)|^2.$$

Define the sequence $\alpha = \alpha_0, \alpha_1, \dots$ by the Newton-Raphson recursion

$$\alpha_{n+1} = \alpha_n - \frac{P(\alpha_n)}{P'(\alpha_n)}.$$

Prove that this sequence converges to a root of P in K . (Hint: show that $|P'(\alpha_{n+1})| = |P'(\alpha_n)|$ but $|P(\alpha_{n+1})|$ is much smaller than $|P(\alpha_n)|$.)

- (b) Apply (a) to recover the fact that any element of $\mathbb{Z}_2$ congruent to 1 modulo 8 is a perfect square, then formulate an analogous statement for any finite extension K of $\mathbb{Q}_2$.
6. (a) Let K be a field equipped with (but not necessarily complete with respect to) a nonarchimedean absolute value $|\cdot|_K$. Let $K(T)$ be the fraction field of the polynomial ring $K[T]$. Prove that there exists a unique absolute value $|\cdot|_G$ on $K(T)$ such that for all $f = \sum_n f_n T^n \in K(T)$,
- $$|f|_G = \max\{|f_n|_K : n = 0, 1, \dots\}.$$
- This is called the Gauss norm on $K(T)$.
- (b) Let L be any field containing K , not necessarily a finite extension. Prove that there exists at least one extension of $|\cdot|_K$ to an absolute value on L . (Hint: using Zorn's lemma, reduce to the case where L is generated over K by a single element α . If α is algebraic over K , use what we proved in class; otherwise, use (a).)